IN THE SPECIFICATION

Please amend the Title on page 1 as follows:

DENIAL-OR-SERVICE ATTACK DEFENSE SYSTEM, DENIAL-OF-SERVICE ATTACK DEFENSE METHOD, AND ~~DENIAL-OF-SERVICE ATTACK DEFENSE PROGRAM~~ COMPUTER PRODUCT

Please replace paragraph [0001] at page 1, lines 8-25, with the following rewritten paragraph:

[0001] The present invention relates to a denial-of-service attack defense system, a denial-of-service attack defense method, and a denial-of-service attack defense program for protecting a communication device against a denial-of-service attack, using a monitoring device that is provided on a ~~LAN~~ local area network (LAN) connected with the communication device as a target of a denial-of-service attack and that monitors a packet transmitted to the communication device via an ~~ISP~~ internal-service-provider (ISP) network, and also using a restricting device that is provided on the ISP network and restricts packets transmitted to the LAN. More particularly, the present invention relates to a denial-of-service attack defense system capable of protecting a communication device against a denial-of-service attack while ensuring privacy of communications and not deviating from a range of its original operations, and also to a denial-of-service attack defense method and a denial-of-service attack defense program.

Please replace paragraph [0002] at page 1, line 28 to page 2, line 14, with the following rewritten paragraph:

[0002] There have been known attacks through networks such as denial-of-service attacks (including distributed denial-of-service attacks). In a denial-of-service attack defense system

that protects communication devices against such denial-of-service attacks, an edge router provided on an ISP ~~(Internet Service Provider)~~ network protects a server machine (hereinafter, "communication device") as a target of an attack. Specifically, to protect a communication device against a SYN flood attack which is one of the denial-of-service attacks, the edge router on the ISP network provides a threshold for a traffic volume of SYN packets, and abandons some SYN packets at an exit of the LAN. More specifically, the ISP network is connected to the LAN ~~(Local Area Network)~~ including the communication device as the target of the attack, the transmission target of the SYN packets is the communication device, and the SYN packets to be abandoned are a portion which exceeds the threshold (see, for example, Patent document 1).

Please replace paragraph [0014] at page 6, lines 20-29, with the following rewritten paragraph:

[0014] According to the present invention, the restricting device further includes a forwarding unit that forwards the protection request information to other restricting device provided on the internet-service-provider network. The forwarding unit determines whether to forward the protection request information based on the report generated [[at]] by the report generating ~~step~~ unit, and forwards the protection request information to the other restricting device upon determining that it is necessary to forward the protection request information.

Please replace paragraph [0015] at page 6, line 30 to page 7, line 7, with the following rewritten paragraph:

[0015] According to the present invention, the restricting device determines whether the protection request information should be forwarded based on the report generated [[at]] by

the report generating ~~step~~ unit, and forwards the protection request information to another restricting device when it is determined that the forwarding is necessary. Therefore, the monitoring device requests the restricting device to remove the passage restriction of the packets which should not be restricted, based on the report. Thus, the passage restriction provided by the restricting device can be made more appropriate.

Please replace paragraph [0038] at page 16, lines 19-29, with the following rewritten paragraph:

[0038] Moreover, according to the present invention, the restricting device determines whether the protection request information should be forwarded based on the report generated [[at]] by the report generating ~~step~~ unit, and forwards the protection request information to another restricting device when it is determined that the forwarding is necessary. Therefore, the monitoring device requests the restricting device to remove the passage restriction of the packets which should not be restricted, based on the report. Thus, the passage restriction provided by the restricting device can be made more appropriate.

Please replace paragraph [0069] at page 27, lines 2-13, with the following rewritten paragraph:

[0069] The protection-request-information forwarding unit 21 determines whether the protection request information transmitted from the monitoring device 5 should be forwarded to other packet restricting device (e.g., the ~~packet~~ restricting devices 8 and 9 of Fig. 1) configured in the same manner as that of the restricting device 6, based on the report generated by the report generating unit 24. When it is determined that the protection request information should be transmitted to the other packet restricting device, the protection-

request-information forwarding unit 21 forwards the protection request information to the other packet restricting device.

Please replace paragraph [0077] at page 29, lines 13-24, with the following rewritten paragraph:

[0077] The protection-request-information forwarding unit 21 determines whether the protection request information received by the communication interface 26 should be forwarded to the other packet restricting device such as the ~~packet~~ restricting devices 8 and 9, based on the report generated by the report generating unit 24 (step S23). When it is determined that the protection request information should be forwarded to the other packet restricting device, the protection-request-information forwarding unit 21 forwards the protection request information to the other packet restricting device (step S24).